



Attorney's Docket No.: UC03-087-4US

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE



MAIL STOP PATENT APPLICATION
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22213-1450

NEW APPLICATION TRANSMITTAL

Transmitted herewith for filing is the patent application of Inventor(s):

PHILLIP ROGAWAY

For (title):

BLOCK CIPHER MODE OF OPERATION FOR CONSTRUCTING A WIDE-BLOCKSIZE BLOCK CIPHER FROM A CONVENTIONAL BLOCK CIPHER

1. Type of Application

(check all applicable)

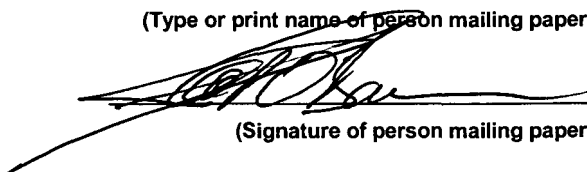
- ☒ Utility
- ☐ Design
- ☐ Plant
- ☐ Divisional
- ☐ Continuation
- ☐ Continuation of PCT designating US
- ☐ Continuation-in-part (CIP)

CERTIFICATION UNDER 37 CFR 1.10

I hereby certify that this New Application Transmittal and the documents referred to as enclosed therein are being deposited with the United States Postal Service on this date 3 SEPTEMBER 2003 in an envelope as "Express Mail Post Office to Addressee" Mailing Label Number EV352305417US addressed to the: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22213-1450.

John P. O'Banion

(Type or print name of person mailing paper)



(Signature of person mailing paper)

NOTE: Each paper or fee referred to as enclosed herein has the number of the "Express Mail" label placed thereon prior to mailing. 37 CFR 1.10(b).

2. Papers Enclosed Which Are Required For Filing Date Under 37 CFR 1.53(b) (Regular) or 37 CFR 1.153 (Design) Application

25 Pages of specification

7 Pages of claims

1 Pages of Abstract

15 Sheets of drawing

X formal

— informal

— The enclosed drawing(s) include photograph(s), and there is also attached a "PETITION TO ACCEPT PHOTOGRAPH(S) AS DRAWING(S)." 37 C.F.R. 1.84(b).

3. Additional papers enclosed

— Preliminary Amendment

— Information Disclosure Statement

— Form PTO - 1449

— Citations

— Authorization of Attorney(s) to Accept and Follow Instructions from Representative

— Special Comments

— Other (SPECIFY)

4. Declaration Or Oath

— Enclosed

executed by:

— inventor(s)

— legal representative of inventor(s). 37 CFR 1.42 or 1.43.

— joint inventor or person showing a proprietary interest on behalf of inventor who refused to sign or cannot be reached.

— this is the petition required by 37 CFR 1.47 and the statement required by 37 CFR 1.47 is also attached. (See item 15 below for fee.)

☐ Copy from a prior application (37 CFR 1.63(d)) (divisional or continuation only)

☒ Not Enclosed. Application is made by a person authorized under 37 CFR 1.41(c) on Behalf of all of the above named inventor(s).

(The declaration or oath, along with the surcharge required by 37 CFR 1.16(e) can be filed subsequently).

5. Inventorship Statement

The inventorship for all the claims in this application are:

☒ The same

or

☐ Are not the same. An explanation, including the ownership of the various claims at the time the last claimed invention was made,

☐ is submitted.

☐ will be submitted.

6. Language

☒ English

☐ non-English

☐ the attached translation is a verified translation. 37 CFR 1.52(d).

7. Assignment

☒ An assignment of the invention to: THE REGENTS OF THE UNIVERSITY OF CALIFORNIA

☐ is attached. A separate "ASSIGNMENT COVER LETTER ACCOMPANYING NEW PATENT APPLICATION" is also attached.

☒ will follow.

8. Benefit of Prior U.S. Application(s) (35 U.S.C. 119(e), 120 or 121)

NOTE: "In order for an application to claim the benefit of a prior filed copending national application, the prior application must name as an inventor at least one inventor named in the later filed application and disclose the named inventor's invention claimed in at least one claim of the later filed application in the manner provided by the first paragraph of 35 U.S.C. 112." 37 CFR 1.78(a).

NOTE: "In addition, the prior application must be (1) complete as set forth in § 1.51, or (2) entitled to a filing date as set forth in § 1.53(b) and include the basic filing fee set forth in § 1.16, or (3) entitled to a filing date as set forth in § 1.53(b) and have paid therein the processing and retention fee set forth in § 1.21(l) within the time set forth in § 1.53(d)." 37 CFR 1.78(a).

NOTE: "Any nonprovisional application claiming the benefit of one or more prior filed copending provisional applications must contain or be amended to contain in the first sentence of the specification following the title a reference to each such prior provisional application, identifying it as a provisional application, and including the provisional application number (consisting of the series code and serial number) and filing date." 37 CFR 1.78(a)(4).

NOTE: "Any nonprovisional application claiming the benefit of one or more prior filed copending nonprovisional applications or international applications designating the United States of America must contain or be amended to contain in the first sentence of the specification following the title a reference to each such prior application, identifying it by application number (consisting of the series code and serial number) and filing date or international application number and international filing date and indicating the relationship of the applications. Cross-references to other related applications may be made where appropriate. (See §1.14(b))." 37 CFR 1.78(2).

X Applicant(s) hereby claim(s) the benefit of the filing date of the following prior U.S. Application(s):

1. Application History (title as originally filed and as last amended, serial number, and filing date of all prior applications):

Title: END MODE OF OPERATION (A TWEAKED, WIDE-BLOCKSIZE, STRONG PRP)
Ser. No.: 60/422,335
Filed: 10/29/2002

Name of applicant(s) (as originally filed and as last amended), and current correspondence address of applicant(s):

Name: PHILLIP ROGAWAY
Address: 1212 PURDUE DRIVE
DAVIS, CA 95616

2. Application History (title as originally filed and as last amended, serial number, and filing date of all prior applications):

Title: EMD BLOCK-CIPHER MODE OF OPERATION GIVING A STRONG PRP
Ser. No.: 60/413,124
Filed: 09/23/2002

Name of applicant(s) (as originally filed and as last amended), and current correspondence address of applicant(s):

Name: PHILLIP ROGAWAY
Address: 1212 PURDUE DRIVE
DAVIS, CA 95616

3. Application History (title as originally filed and as last amended, serial number, and filing date of all prior applications):

Title: BLOCK-CIPHER MODE OF OPERATION GIVING A STRONG PRP
Ser. No.: 60/408,458
Filed: 09/03/2002

Name of applicant(s) (as originally filed and as last amended), and current correspondence address of applicant(s):

Name: PHILLIP ROGAWAY
Address: 1212 PURDUE DRIVE
DAVIS, CA 95616

NOTE: The proper reference to a prior filed PCT application which entered the U.S. national phase is the U.S. serial number and the filing date of the PCT application which designated the U.S.

NOTE: (1) Where the application being transmitted adds subject matter to the International Application then the filing can be as a continuation-in-part or (2) it is desired to do so for other reasons, then the filing can be as a continuation.

NOTE: The deadline for entering the national phase in the U.S. for an international application was clarified in the Notice of April 28, 1987 (1079 O.G. 32 to 46) as follows:

"The Patent and Trademark Office considers the international application to be pending until the 22nd month from the priority date if the United States has been designated and no Demand for International Preliminary Examination has been filed prior to the expiration of the 19th month from the priority date and until the 32nd month from the priority date if a Demand for International Preliminary Examination which elected the United States of America has been filed prior to the expiration of the 19th month from the priority date, provided that a copy of the international application has been communicated to the Patent and Trademark Office within the 20 or 30 month period respectively. If a copy of the international application has not been communicated to the Patent and Trademark Office within the 20 or 30 month period, respectively, the international application becomes abandoned as to the United States 20 or 30 months from the priority date, respectively. These periods have been placed in the rules as paragraph (h) of § 1.494 and paragraph (i) of § 1.495. A continuing application under 35 U.S.C. 365(c) and 120 may be filed anytime during the pendency of the international application."

9. Priority Claim for Prior Application (35 U.S.C. 119)

_____ The prior U.S. application(s), including any prior International Application designating the U.S. identified above in item 8, in turn itself claim(s) foreign priority (ies) as follows:

_____ (country)	_____ (appln. no.)	_____ (filed on)
_____ (country)	_____ (appln. no.)	_____ (filed on)
_____ (country)	_____ (appln. no.)	_____ (filed on)

The certified copy (ies)

_____ is (are) attached.

_____ has (have) been filed on _____ in prior application serial number _____ which was filed on _____.

_____ will follow.

WARNING: The certified copy of the priority application which may have been communicated to the PTO by the International Bureau may not be relied on without the need to file a certified copy of the priority application in a continuing application. This is so because the certified copy of the priority application communicated by the International Bureau is placed in a folder and is not assigned a U.S. serial number unless the national stage is entered. Such folders are disposed of if the national stage is not entered. Therefore, such certified copies may not be available if needed later in the prosecution of a continuing application. An alternative would be to physically remove the priority documents from the folders and transfer them to the continuing application. The resources required to request transfer, retrieve the folders, make suitable record notations, transfer the certified copies, enter and make a record of such copies in the continuing application are substantial. Accordingly, the priority documents in folders of international applications which have not entered the national stage may not be relied on. Notice of April 28, 1987 (1079 O.G. 32 to 46).

10. Further Inventorship Statement Where Benefit of Prior Application(s) Claimed

NOTE: "If the continuation, continuation-in-part, or divisional application is filed by less than all the inventors named in the prior application, a statement must accompany the application when filed requesting deletion of the names of the person or persons who are not inventors of the invention being claimed in the continuation, continuation-in-part, or divisional application." 37 CFR 1.62(a) [emphasis added] (dealing with the file wrapper continuation situation).

NOTE: "In the case of a continuation-in-part application which adds and claims additional disclosure by amendment, an oath or declaration as required by § 1.63 must be filed. In those situations where a new oath or declaration is required due to

additional subject matter being claimed, additional inventors may be named in the continuing application. In a continuation or divisional application which discloses and claims only subject matter disclosed in a prior application, no additional oath or declaration is required and the application must name as inventors the same or less than all the inventors in the prior application." 37 CFR 1.60(c). (dealing with the continuation situation).

(complete applicable item (a) or (b) below)

(a) ☐ This application discloses and claims only subject matter disclosed in the prior application whose particulars are set out above and the inventor(s) in this application are

☐ the same

☐ less than those named in the prior application and it is requested that the following inventor(s) identified above for the prior application be deleted:

Name:

Name:

Name:

(b) ☐ This application discloses and claims additional disclosure and a new declaration or oath is being filed. With respect to the prior application whose particulars are set out above, the inventors in this application are

☐ the same

☐ add the following inventors

Name:

Name:

Name:

11. Maintenance of Copendency of Prior Application

NOTE: The PTO finds it useful if a copy of the petition filed in the prior application extending the term for response is filed with the papers constituting the filing of the continuation application. Notice of November 5, 1985 (1060 O.G. 27).

☐ Extension of time in prior application

(This item must be completed and the necessary papers filed in the prior application if the period set in the prior application has run)

☐ A petition, fee and response has been filed to extend the term in the prior application until _____.

☐ A copy of the petition for extension of time in the prior application is attached.

(complete this item and file conditional petition in prior application if previous item not applicable)

☐ Conditional Petition For Extension Of Time In Prior Application

☐ A conditional petition for extension of time is being filed in the pending prior application.

12. Fee Calculation (37 CFR 1.16)**A. X Regular Application**

CLAIMS AS FILED									
		Number filed		Number Extra		Rate		Basic Fee \$ 750.00	
Total									
Claims 37 CFR 1.16(c)		47	- 20	=	27	X	\$18.00	=	486.00
Independent									
Claims (37 CFR 1.16(b))		12	- 3	=	9	X	\$84.00	=	756.00
Multiple dependent claim(s), if any (37 CFR 1.16(d))						+	\$280.00	=	

- ☐ Amendment canceling extra claims enclosed.
- ☐ Amendment deleting multiple-dependencies enclosed.
- ☐ Fee for extra claims is not being paid at this time.

Filing Fee Calculation \$ 1992.00

B. ☐ Design application
(\$330.00 - 37 CFR 1.16(f))

Filing Fee Calculation \$ _____

C. ☐ Plant application
(\$520.00 - 37 CFR 1.16(g))

Filing Fee Calculation \$ _____

13. Small Entity Statement

X Applicant qualifies as a small entity under 37 CFR 1.9 and 1.27

Filing Fee Calculation (50% of **A**, **B** or **C** above) \$ 996.00

14. Request for International-Type Search (37 CFR 1.104(d))

- ☐ Please prepare an international-type search report for this application at the time when national examination on the merits takes place.

15. Fee Payment Being Made At This Time

X Not Enclosed

X No filing fee is to be paid at this time. (This and the surcharge required by 37 CFR 1.16(e) can/will be paid subsequently.)

☐ Enclosed

☐ basic filing fee \$ _____

☐ recording assignment (\$40.00; 37 CFR 1.21(h)) \$ _____

☐ petition fee for filing by other than all the

	inventors or person on behalf of the inventor where inventor refused to sign or cannot be reached. (\$130.00; 37 CFR 1.47 and 1.17(h))	\$ _____
—	for processing an application with a specification in a non-English language. (\$130.00; 37 CFR 1.52(d) and 1.17(k))	\$ _____
—	processing and retention fee (\$130.00; 37 CFR 1.53(d) and 1.21(l))	\$ _____
—	fee for international-type search report. (\$40.00; 37 CFR 1.21(e))	\$ _____
	Total Fees Enclosed	\$ _____

16. Method of Payment of Fees

— Check in the amount of \$ _____

— Charge Account No. _____ in the amount of \$ _____.
A duplicate of this transmittal is attached.

17. Authorization to Charge Additional Fees

— The Commissioner is hereby authorized to charge the following additional fees by this
paper and during the entire pendency of this application to Account No. _____;

— 37 CFR 1.16(a), (f) or (g) (filing fees)

— 37 CFR 1.16(b), (c) and (d) (presentation of extra claims)

— 37 CFR 1.16(e) (surcharge for filing the basic filing fee and/or declaration on a
date later than the filing date of the application)

— 37 CFR 1.18 (application processing fees)

— 37 CFR 1.18 (issue fee at or before mailing of Notice of Allowance, pursuant to
37 CFR 1.311(b))

18. Instructions As To Overpayment

— credit Account No. _____

X refund

19. Incorporation By Reference of Papers Identified Herein

Applicant(s) hereby incorporate(s) by reference all papers which are identified in this New
Application Transmittal.

20. Correspondence Address

Please use the following correspondence address for all communications:

John P. O'Banion, Reg. No. 33,201
O'BANION & RITCHEY LLP
400 Capitol Mall, Suite 1550
Sacramento, CA 95814
(916) 498-1010

CUSTOMER NUMBER 8156




8156

PATENT TRADEMARK OFFICE

21. Signature of Attorney

Dated: 9/3/03


SIGNATURE OF ATTORNEY
John P. O'Banion, Reg. No. 33,201
CUSTOMER NUMBER 8156

CERTIFICATION UNDER 37 CFR 1.10

I hereby certify that the foregoing

U.S. Patent Application

1. Specification (pages 1-25)
2. Claims (pages 26-32)
3. Abstract (page 33)
4. Drawings (sheets 1-15)

is being deposited with the United States Postal Service on 3 SEPTEMBER 2003
in an envelope as "Express Mail Post Office to Addressee" Mailing Label Number
EV352305417US addressed to the: Commissioner for Patents, P.O. Box 1450,
Alexandria, VA 22313-1450.

JOHN P. O'BANION

(Type or print name of person mailing paper)


(Signature of person mailing paper)